simplifi

End user qualified certificate profile

Profiles and parameters for qualified certificates issued under eIDAS and ETSI standards

This document defines the qualified certificate profiles used by Simplifi as a Qualified Trust Service Provider (QTSP). It covers the structure and parameters for end-user Qualified Electronic Signatures (QES), QES certificates for natural persons acting on behalf of legal persons, and Qualified Electronic Seals. In addition, it specifies supporting profiles for OCSP responder and CRL issuance.

Each profile is aligned with eIDAS and ETSI EN 319 standards, detailing subject naming conventions, key usage, validity periods, certificate policies, and mandatory extensions such as QCStatements and PDS references. Distribution points for CRLs, OCSP, and AIA are included to ensure interoperability and compliance.

The objective is to provide consistent, standards-based certificates that support remote signing, seal creation, and revocation services, while ensuring long-term legal validity and trust across the European Union.

Document information

Version	1.0
Version Date	September 1st, 2025
Approved by	CEO
Owner of the Document	Trust Service Manager
Document Name	End user qualified certificate profile
Document OID	1.3.6.1.4.1.63578.1.5.1
Document Classification	Public

Document history

Version	Effective Date	Reason	Author
V 1.0	2025-09-01	Initial publishing	Trust Service Manager

Approval history

Version	Approval Date	Approver Name
V 1.0	2025-09-01	CEO

Distribution history

Version	Distribution Date	Distribution
V 1.0	2025-09-01	Trust Service Manager

Contents

1. Introduction

The document describes profile for certificates for electronic signatures issued by Simplifi. Also relevant CRL-s profiles.

2. Technical profile of certificate

Certificate is compiled in accordance with the X.509 version 3, IETF RFC 5280, ETSI EN 319 412-2 and ETSI EN 319 411-2

3. Certificate body

3.1. Qualified Electronic Signature Certificate

The following table gives the Certificate profile and extensions.

Qualified Electronic Signature (long term)			
Field	Mandatory	Value	Description
Certificate data			
Serial number	Yes	<unique_serial_number>	Unique random assigned by CA
Version	Yes	3	
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Issuer DN			
Common Name (CN)	Yes	Simplifi Qualified CA Class 3 [XX]	Certificate authority name, where [XX] is G1,G2,G3…
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Subject DN			
Common Name (CN)	Yes	<common_name>	Subject common name in Latin letters.
Given Name (GN)	Yes	<given_name>	Subject given name in Latin letters.
Surname (SN)	Yes	<surname>	Subject surname in Latin letters.

Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Serial Number (SN)	Yes	<serial_number>	As per ETSI EN 319 412-1 v1.4.4, section 5.1.3, Semantics Identifier for natural persons. Identifier for a natural person is for example: - PNORO-1234567890123 or IDCRO-DZ123456 or TINRO-1234567890123 for identification based on Carte de Identitate Electronică Code
Validity			
Validity period	Yes	3 years	Validity period of certificate from issuance date.
Not before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + 3 years	Last date of certificate validity.
Public key info			
Algorithm	Yes	RSA (2048 Bits)	RSA algorithm in accordance with RFC 4055
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extensions	**Values and limitations**	**Criticality**	**Mandatory**
Key Usage	Non-repudiation, digitalSignature	Critical	Yes
Basic Constraints	Subject Type = End Entity	Critical	Yes
Subject Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	Non-critical	Yes
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Authority Information Access	Method #1: CA issuer:	Non-critical	Yes

	http://Simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp		
CRL Distribution Points	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-critical	Yes
Subject Alternative Name			
822Name	Subject email address	Non-critical	Yes
qcStatement			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.1 (qcSemanticsIdNatural)	Non-critical	Yes
id-etsi-qcs-QcCompliance	Yes	Non-critical	Yes
id-etsi-qcs-QcSSCD	Private key resides in a QSCD	Non-critical	Yes
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds language=en	Non-critical	Yes
id-etsi-qcs-QcType	id-etsi-qct-esign	Non-critical	Yes

3.2. Qualified Certificates for Electronic Signature (natural person representing legal person)

The following table gives the Certificate profile and extensions.

Qualified Electronic Signature (long term)			
Field	Mandatory	Value	Description
Certificate data			
Serial number	Yes	<unique_serial_number>	Unique random assigned by CA
Version	Yes	3	
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Issuer DN			

Common Name (CN)	Yes	Simplifi Qualified CA Class 3 [XX]	Certificate authority name, where [XX] is G1,G2,G3…
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Subject DN			
Common Name (CN)	Yes	<common_name>	Subject common name in Latin letters.
Given Name (GN)	Yes	<given_name>	Subject given name in Latin letters.
Surname (SN)	Yes	<surname>	Subject surname in Latin letters.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Serial Number (SN)	Yes	<serial_number>	As per ETSI EN 319 412-1 v1.4.4, section 5.1.3, Semantics Identifier for natural persons. Identifier for a natural person is for example: - PNORO-1234567890123 or IDCRO-DZ123456 or TINRO-1234567890123 for identification based on Carte de Identitate Electronică Code
Organization (O)	Yes	<organization_name>	Organization name associated with the natural person.
Organization Identifier (ORGID)	Yes	<orgid>	Organization identifier associated with the natural person. Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Validity			
Validity period	Yes	3 years	Validity period of certificate from issuance date.
Not before	Yes	<issuance_date_and_time>	First date of certificate validity.

Not After	Yes	<issuance_date_and_time> + 3 years	Last date of certificate validity.
Public key info			
Algorithm	Yes	RSA (2048 Bits)	RSA algorithm in accordance with RFC 4055
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extensions	**Values and limitations**	**Criticality**	**Mandatory**
Key Usage	Non-repudiation, digitalSignature	Critical	Yes
Basic Constraints	Subject Type = End Entity	Critical	Yes
Subject Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	Non-critical	Yes
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Authority Information Access	Method #1: CA issuer: http://Simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp	Non-critical	Yes
CRL Distribution Points	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-critical	Yes
Subject Alternative Name			
822Name	Subject email address	Non-critical	Yes
qcStatement			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.1 (qcSemanticsIdNatural)	Non-critical	Yes

id-etsi-qcs-QcCompliance	Yes	Non-critical	Yes
id-etsi-qcs-QcSSCD	Private key resides in a QSCD	Non-critical	Yes
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds language=en	Non-critical	Yes
id-etsi-qcs-QcType	id-etsi-qct-esign	Non-critical	Yes

3.3. Qualified Electronic Seal Certificate

Qualified Electronic Signature (long term)			
Field	Mandatory	Value	Description
Certificate data			
Serial number	Yes	<unique_serial_number>	Unique random assigned by CA
Version	Yes	3	
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Issuer DN			
Common Name (CN)	Yes	Simplifi Qualified CA Class 3 [XX]	Certificate authority name, where [XX] is G1,G2,G3…
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)

Common Name (CN)	Yes	<common_name>	The organization name
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)

Organization (O)	Yes	<organization_name>	Legal entity name for which the qualified electronic seal certificate is issued.
Organization Identifier (ORGID)	Yes	<orgid>	Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Validity			
Validity period	Yes	3 years	Validity period of certificate from issuance date.
Not before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + 3 years	Last date of certificate validity.
Public key info			
Algorithm	Yes	RSA (2048 Bits)	RSA algorithm in accordance with RFC 4055
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extensions	**Values and limitations**	**Criticality**	**Mandatory**
Key Usage	Non-repudiation, digitalSignature	Critical	Yes
Basic Constraints	Subject Type = End Entity	Critical	Yes
Subject Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Certificate Policies	Certificate Policy [1]: PolicyIdentifier: 0.4.0.194112.1.2 Certificate Policy [2]: PolicyIdentifier: 1.3.6.1.4.1.63578.1.1.1 CPS URI: http://simplifi.ro/policies	Non-critical	Yes
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Authority Information Access	Method #1: CA issuer:	Non-critical	Yes

	http://Simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crt Method #2: OCSP: http://simplifi.ro/ocsp		
CRL Distribution Points	http://simplifi.ro/pki/Simplifi_Qualified_CA_Class_3_G1.crl	Non-critical	Yes
qcStatement			
id-qcs-pkixQCSyntax-v2	0.4.0.194121.1.2 (qcSemanticsIdLegal)	Non-critical	Yes
id-etsi-qcs-QcCompliance	Yes	Non-critical	Yes
id-etsi-qcs-QcSSCD	Private key resides in a QSCD	Non-critical	Yes
id-etsi-qcs-QcPDS	http://simplifi.ro/policies/pds language=en	Non-critical	Yes
id-etsi-qcs-QcType	id-etsi-qct-eseal	Non-critical	Yes

4. OCSP Profile

OCSP			
Field	**Mandatory**	**Value**	**Description**
Certificate data			
Serial number	Yes	<unique_serial_number>	Unique random assigned by CA
Version	Yes	3	
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Issuer DN			
Common Name (CN)	Yes	Simplifi Qualified CA Class 3 {XX]	Certificate authority name, where [XX] is G1,G2,G3…
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name.

			3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Subject DN			
Common Name (CN)	Yes	Simplifi Qualified CA Class 3 [G1] OCSP	Common name of OCSP
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Validity			
Validity period	Yes	1 year	Validity period of certificate from issuance date.
Not before	Yes	<issuance_date_and_time>	First date of certificate validity.
Not After	Yes	<issuance_date_and_time> + year	Last date of certificate validity.
Public key info			
Algorithm	Yes	RSA (2048 Bits)	RSA algorithm in accordance with RFC 4055
Public Key	Yes	<public_key>	Public Key.
Extensions			
Extensions	**Values and limitations**	**Criticality**	**Mandatory**
Key Usage	Digital Signature	Critical	Yes
Extended Key Usage	OCSP Signer	Non-critical	Yes
Basic Constraints	Subject Type = End Entity	Critical	Yes
Subject Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
OCSP No Check		Non-critical	Yes

5. CRL Profile

CRL			
Field	**Mandatory**	**Value**	**Description**

CRL data			
Version	Yes	2	CRL format version pursuant to X.509.
Signature Algorithm	Yes	SHA512	Signature algorithm in accordance to RFC 5280.
Expire Period	Yes	7 days	Time interval during which CRL is valid.
Issue Interval	Yes	1 day	Time interval during which CRL is generated and published
Overlap Time	Yes	0 minutes	Time interval during which both old and new CRLs are valid.
Issuer DN			
Common Name (CN)	Yes	Simplifi Qualified CA Class 3 {XX]	Certificate authority name, where [XX] is G1,G2,G3…
Organization (O)	Yes	SIMPLIWORKS SRL	Organization name
Organization Identifier (ORGID)	Yes	VATRO-45938180	Identification of the organization different from the organization name. 3 characters+Country ID+ Identifier as per ETSI EN 319 412-1 v1.4.4, section 5.1.4, semantics identifier for legal person.
Country (C)	Yes	RO	Country code: RO – Romania (2 character ISO 3166 country code)
Extensions			
Extensions	**Values and limitations**	**Criticality**	**Mandatory**
Authority Key Identifier	160-bit SHA-1 hash (Key ID)	Non-critical	Yes
CRL Number	Digit starts from number 1	Non-critical	Yes